SecAware case study

ISO 27001 ISMS

•

Internal Audit

Client situation

A New Zealand engineering/Operational Technology support services company needed an internal audit of its shiny new ISO/IEC 27001 **I**nformation **S**ecurity **M**anagement **S**ystem before the certification audit, due just a few weeks later.

The company had a keen interest in cybersecurity and planned on using its ISO/IEC 27001 certificate to promote its information security-related services, supplying and extending its customer base. Management was sufficiently concerned about protecting the company's own information plus customer data in its care to invest in the ISMS as an integral part of its business strategy.

www.SecAware.com

Consulting assignment

We were appointed to:

- Conduct an internal audit of the ISMS in accordance with ISO/IEC 27001:2013 clause 9.2;
- Examine and evaluate evidence relating to and generated by the ISMS;
- Review and comment on the alignment of the ISMS with the requirements in the standard and broader organisational/business objectives for information risk and security management;
- Prepare, present and discuss the raw findings with the client's senior management;
- Deliver a formal internal audit report with the findings, recommendations and supporting evidence.

Outcome

With just 7 consulting days available, though, the audit was necessarily at a fairly high level given the wide scope. Thankfully, the client had adopted ISO/IEC 27001 Annex A controls, hence we were able to use our standard Internal Controls Questionnaires covering the main body clauses and Annex A controls.

The audit identified strengths, weaknesses, opportunities and threats – a classic SWOT analysis of the evidence collected during the audit fieldwork.

We recommended improvements to the ISMS governance and management arrangements, pointing out specific changes required for conformity with ISO/IEC 27001. There was a need to launch and start operating the ISMS.

Lessons learnt

- Although the client was heavily into customers' OT (process control) systems, its own information risks and controls mostly involved conventional corporate IT.
- Thanks to its OT expertise, managers and staff were familiar with system engineering plus risk and security management, and were clearly committed to this.
- Some realignment of the ISMS and its governance arrangements was required to conform more directly with the mandatory requirements of the standard, and to generate various security procedures and process records demonstrating that the ISMS and the controls were in full operation prior to the certification audit.
- Additional recommendations included explicitly allocating important information risk and security management responsibilities among employees, addressing information risks associated with professional services, and developing appropriate metrics.

Management accepted the findings … and the company was successfully certified as planned.

Find out more about us on the SecAware and IsecT websites. Read about ISO/IEC 27001 and the other ISO27k standards at ISO27001security.com. Email us at info@isect.com.

IsecT Limited, Castle Peak, 1262 Taihape Road, Hastings, New Zealand

Call/text +64 21 16 55 33 5 during NZ office hours